

# ON THE REDUCIBILITY TYPE OF TRINOMIALS

ANDREW BREMNER (TEMPE) AND MACIEJ ULAS (KRAKÓW)

ABSTRACT. Say a trinomial  $x^n + Ax^m + B \in \mathbb{Q}[x]$  has reducibility type  $(n_1, n_2, \dots, n_k)$  if there exists a factorization of the trinomial into irreducible polynomials in  $\mathbb{Q}[x]$  of degrees  $n_1, n_2, \dots, n_k$ , ordered so that  $n_1 \leq n_2 \leq \dots \leq n_k$ . Specifying the reducibility type of a monic polynomial of fixed degree is equivalent to specifying rational points on an algebraic curve. When the genus of this curve is 0 or 1, there is reasonable hope that all its rational points may be described; and techniques are available that may also find all points when the genus is 2. Thus all corresponding reducibility types may be described. These low genus instances are the ones studied in this paper.

2010 *Mathematics Subject Classification*: Primary 11R09; Secondary 11C08, 12E10, 14G05

*Key words and phrases*: trinomial, reducibility

## 1. INTRODUCTION

The reducibility over  $\mathbb{Q}$  of trinomials  $x^n + Ax^m + B \in \mathbb{Q}[x]$ ,  $AB \neq 0$  (where without loss of generality  $n \geq 2m$ ), has a long history, and the reader is referred to Schinzel [3], reprinted in Schinzel [6], who provides an excellent documentation and full bibliography. Here, we study the *type* of reducibility of trinomials. We say a trinomial has reducibility type  $(n_1, n_2, \dots, n_k)$  if there exists a factorization of the trinomial into irreducible polynomials in  $\mathbb{Q}[x]$  of degrees  $n_1, n_2, \dots, n_k$ . Types are ordered so that  $n_1 \leq n_2 \leq \dots \leq n_k$ . Thus, for example,

$$x^5 - 341x + 780 = (x - 3)(x^2 + x + 20)(x^2 + 2x - 13)$$

has reducibility type  $(1, 2, 2)$ . We consider trinomials only up to scaling, in that the polynomials  $x^n + Ax^m + B$  and  $x^n + A\lambda^{n-m}x^m + B\lambda^n$ ,  $\lambda \in \mathbb{Q}$ , have exactly the same factorization type; in particular, when the trinomial has a rational root, we may assume that this root is 1. We shall always assume  $AB \neq 0$ .

A monic polynomial of degree  $d$  is determined by  $d$  coefficients. Specify the reducibility type of  $x^n + Ax^m + B$  as  $(d_1, d_2, \dots, d_k)$ ; then comparing coefficients of  $x^r$ ,  $1 \leq r < n$ ,  $r \neq m$ , leads to  $n - 2$  equations involving  $\sum_{i=1}^k d_i = n$  coefficients. With the appropriate weighting of the coefficients, the variety so determined has generic dimension 1 in weighted projective space, so is a curve. When the genus of this curve is 0 or 1, there is reasonable hope that all its rational points may be described; and techniques are available that may also find all points when the genus is 2. These low genus instances are the ones we investigate in this paper.

Although our motivation is the reducibility of trinomials over  $\mathbb{Q}$  it is clear that the

constructions of curves related to a particular type of reducibility can be viewed over other fields (of characteristic 0).

It is immediate to verify the following. The quadratic  $x^2 + Ax + B \in \mathbb{Q}[x]$  is reducible, so of type (1, 1), if and only if up to scaling  $(A, B) = (u - 1, -u)$ , for  $u \in \mathbb{Q} \setminus \{0, 1\}$ . A cubic  $x^3 + Ax + B$  is of type (1, 2) if and only if up to scaling  $(A, B) = (u - 1, -u)$ , for  $u \in \mathbb{Q} \setminus \{0, 1\}$  and  $-4u + 1 \neq \square$ ; and is of type (1, 1, 1) if and only if  $(A, B) = (-v^2 + v - 1, v^2 - v)$ , for  $v \in \mathbb{Q} \setminus \{0, 1\}$ .

## 2. REDUCIBILITY TYPE OF QUARTIC TRINOMIALS

**Theorem 2.1.** *The trinomial  $x^4 + Ax + B$  has reducibility type (1, 1, 2) if and only if up to scaling*

$$A = -(u + 1)(u^2 + 1), \quad B = u(u^2 + u + 1), \quad u \in \mathbb{Q} \setminus \{0, -1\},$$

*with factorization*

$$x^4 + Ax + B = (x - 1)(x - u)(x^2 + (u + 1)x + (u^2 + u + 1)).$$

*There are no polynomials  $x^4 + Ax + B$  with reducibility type (1, 1, 1, 1).*

*Proof.* Suppose we have reducibility type (1, 1, 2). By scaling, there is a linear factor  $x - 1$ , and  $x^4 + Ax + B = (x - 1)(x - u)(x^2 + px + q)$ . On comparing coefficients of powers of  $x$ ,

$$p - u - 1 = 0, \quad q - pu - p + u = 0, \quad A = -qu - q + pu, \quad B = qu,$$

and thus

$$p = u + 1, \quad q = u^2 + u + 1, \quad (A, B) = (-(u + 1)(u^2 + 1), u(u^2 + u + 1)),$$

as required. The discriminant of the quadratic factor is  $-3u^2 - 2u - 3 < 0$ , so that reducibility type (1, 1, 1, 1) is impossible.  $\square$

**Theorem 2.2.**  *$x^4 + Ax^2 + B$  has reducibility type (1, 1, 2) if and only if up to scaling*

$$(A, B) = (q - 1, -q), \quad q \in \mathbb{Q} \setminus \{1\}, \quad -q \neq \square;$$

*with factorization*

$$x^4 + Ax^2 + B = (x - 1)(x + 1)(x^2 + q);$$

*and has reducibility type (1, 1, 1, 1) if and only if*

$$(A, B) = (-u^2 - 1, u^2), \quad u \in \mathbb{Q} \setminus \{0\},$$

*with factorization*

$$x^4 + Ax^2 + B = (x - 1)(x + 1)(x - u)(x + u).$$

*Proof.* By scaling, suppose  $x^4 + Ax^2 + B = (x - 1)(x - u)(x^2 + px + q)$ ; then equating coefficients of powers of  $x$ :

$$p - u - 1 = 0, \quad A = q - pu - p + u, \quad -qu - q + pu = 0, \quad B = qu.$$

It follows that  $p(q - u) = 0$ . If  $p = 0$  then  $u = -1$  and  $(A, B) = (q - 1, -q)$ ; and if  $q = u$ , then  $(A, B) = (-u^2 - 1, u^2)$ .  $\square$

## 3. REDUCIBILITY TYPE OF QUINTIC TRINOMIALS

**Theorem 3.1.** *The trinomial  $x^5 + Ax + B$  has reducibility type  $(1, 2, 2)$  if and only if up to scaling*

$$A = \frac{(v^2 - v - 1)(v^4 - 2v^3 + 4v^2 - 3v + 1)}{(2v - 1)^2},$$

$$B = -\frac{v(v - 1)(v^2 + 1)(v^2 - 2v + 2)}{(2v - 1)^2}$$

for  $v \in \mathbb{Q}$  with  $v \neq 0, 1, 1/2$ . There are no trinomials  $x^5 + Ax + B$  with reducibility type  $(1, 1, 1, 2)$ .

*Proof.* By scaling we suppose the linear factor  $x - 1$ , with

$$x^5 + Ax + B = (x - 1)f_1(x)f_2(x) = (x - 1)(x^2 + px + q)(x^2 + vx + w).$$

Comparing coefficients of powers of  $x$ , we get the system of equations

$$\begin{aligned} p + v - 1 &= 0, & (v - 1)p + q - v + w &= 0, & (v - w)p - (v - 1)q + w &= 0, \\ A + pw + (v - w)q &= 0, & B + qw &= 0. \end{aligned}$$

Solving for  $p, q, w, A, B$  we get  $A, B$  as given in the statement of the Theorem and

$$p = 1 - v, \quad q = \frac{v(v^2 - 2v + 2)}{2v - 1}, \quad w = \frac{(v - 1)(v^2 + 1)}{2v - 1}.$$

It remains to show that the quadratics  $f_i(x)$  are irreducible. Without loss of generality, we show that  $f_2(x)$  is irreducible. The discriminant of  $f_2(x)$  is  $v^2 - 4w = -(2v^3 - 3v^2 + 4v - 4)/(2v - 1)$ , so  $f_2(x)$  is reducible if and only if

$$-(2v - 1)(2v^3 - 3v^2 + 4v - 4) = 0.$$

This latter is the equation of an elliptic curve with minimal model  $y^2 + xy + y = x^3 - x - 2$ , and rank 0 over  $\mathbb{Q}$ . The torsion group is of order 3, whose points lead to  $AB = 0$ . Hence there is no non-trivial specialization of  $v$  which leads to the reducibility of  $f_2(x)$ , and the Theorem follows.  $\square$

**Theorem 3.2.** *There are no trinomials  $x^5 + Ax^2 + B$  with reducibility type  $(1, 2, 2)$  or  $(1, 1, 1, 2)$ .*

*Proof.* By scaling, suppose that  $x^5 + Ax^2 + B = (x - 1)(x^2 + px + q)(x^2 + rx + s)$ . Equating coefficients of  $x^4, x^3, x$ :

$$p + r - 1 = 0, \quad q + pr + s - p - r = 0, \quad qs - qr - ps = 0.$$

On eliminating  $r, s$ , it follows that

$$q^2 - q(p + p^2) + p - p^2 + p^3 = 0,$$

whence

$$(p + p^2)^2 - 4(p - p^2 + p^3) = 0,$$

the equation of an elliptic curve with minimal model  $y^2 + xy + y = x^3 + x^2$ , of rank 0, and with torsion group  $\mathbb{Z}/4\mathbb{Z}$ , generated by  $(x, y) = (0, 0)$ . The four torsion points lead to  $B = 0$ .  $\square$

**Corollary 3.3.** *The equation (representing a curve of genus 3)*

$$G(p, q, r) : (p + q)(q + r)(r + p)(p + q + r) - (pq + qr + rp)^2 = 0$$

*has only trivial rational solutions i.e. those with  $pqr = 0$ .*

*Proof.* Suppose  $G(p, q, r) = 0$  with  $pqr \neq 0$ . Certainly the absolute values of  $p, q, r$  are distinct. For if, without loss of generality,  $p = q$ , then  $q(3q^3 + 6q^2r + 4qr^2 + 2r^3) = 0$ , so that  $q = 0$ ; and if  $p = -q$ , then  $q^4 = 0$ , and again  $q = 0$ . Consider the trinomial

$$H(X) = X^5 - \frac{p^5 - q^5}{p^2 - q^2}X^2 + \frac{p^2q^2(p^3 - q^3)}{p^2 - q^2}.$$

We have  $H(p) = H(q) = 0$  and  $H(r) = (p - r)(q - r)G(p, q, r)/(p + q) = 0$ . This contradicts Theorem 3.2, since there are no trinomials  $x^5 + Ax^2 + B$  with three rational roots.  $\square$

#### 4. REDUCIBILITY TYPE OF SEXTIC TRINOMIALS

**Theorem 4.1.** *There are infinitely many trinomials  $x^6 + Ax + B$  with reducibility type  $(1, 2, 3)$ . There are no trinomials  $x^6 + Ax + B$  with reducibility type  $(1, 1, 1, 3)$ .*

*Proof.* By scaling, suppose that  $x^6 + Ax + B = (x - 1)(x^2 + vx + w)(x^3 + px^2 + qx + r)$ . Equating coefficients of  $x^5, \dots, x^2$ :

$$\begin{aligned} p + v - 1 &= 0, & q - p + pv - v + w &= 0, & r - q + qv - pv + pw - w &= 0, \\ -r + rv - qv + qw - pw &= 0; \end{aligned}$$

and eliminating  $p, q, r$ :

$$(1) \quad (3v^2 - 2v + 1 - 2w)^2 = (v - 1)(5v^3 - 3v^2 + 3v + 3).$$

This latter is the equation of an elliptic curve  $E$  with minimal model  $y^2 = x^3 + 3x + 1$ , of rank 1 with generator  $P(x, y) = (0, 1)$ . Each multiple of  $P$  pulls back to a trinomial of type  $x^6 + Ax + B$  factoring into polynomials of degrees 1, 2, 3. Now if the quadratic is reducible, then  $v^2 - 4w = \square$ , which with (1) represents a curve of genus 3, so having only finitely many points  $v, w$ . The cubic factoring together with (1) represents a curve of genus 7 and so again, there are only finitely many points  $(v, w)$ . Since the number of points on  $E$  is infinite, all but finitely many such points lead to trinomials with reducibility type  $(1, 2, 3)$ . As an example, the point  $2P = (9/4, -35/8)$  pulls back to the trinomial

$$x^6 - 19656x + 82655 = (x - 5)(x^2 + 13x + 61)(x^3 - 8x^2 + 68x - 271).$$

The second assertion of the Theorem follows from Theorem 7.1 below.  $\square$

**Theorem 4.2.** *There are no trinomials  $x^6 + Ax + B$  with reducibility type  $(1, 1, 2, 2)$  or  $(2, 2, 2)$ .*

*Proof.* Suppose  $x^6 + Ax + B = (x^2 + px + q)(x^2 + rx + s)(x^2 + ux + v)$ . Equating coefficients of  $x^5, \dots, x^2$ :

$$\begin{aligned} -p - r - u &= 0, & -p(u + r) - q - ur - s - v &= 0, \\ -(s + ru + v)p - (r + u)q - vr - us &= 0, & -(su + rv)p - (s + ru + v)q - vs &= 0, \end{aligned}$$

and eliminating  $p, q, s$  results in

$$\begin{aligned} 3(r^2 + ru + u^2)v^2 + 2(r^4 + 2r^3u - 3r^2u^2 - 4ru^3 - 2u^4)v \\ - (r^6 + 3r^5u + 5r^4u^2 + 5r^3u^3 - 2ru^5 - u^6) &= 0. \end{aligned}$$

The discriminant in  $v$  must be a perfect square, leading to

$$(2r + u)^2(r^6 + 3r^5u + 3r^4u^2 + r^3u^3 + 3r^2u^4 + 3ru^5 + u^6) = \square.$$

The restriction  $u = -2r$  leads to trivial solutions, and thus  $(X, Z) = (u + 2r, u)$  gives a point on the genus 2 curve

$$C : Y^2 = X^6 - 3X^4Z^2 + 51X^2Z^4 + 15Z^6.$$

$C$  covers two obvious elliptic curves,

$$E_1 : y^2 = x^3 - 3x^2 + 51x + 15, \quad E_2 : y^2 = 15x^3 + 51x^2 - 3x + 1,$$

but each  $E_i$  is of rank 1 over  $\mathbb{Q}$ , so there is no simple way to compute the finitely many rational points on  $C$ . However, we can argue as follows, and show that the only rational points on  $C$  are  $(\pm X, \pm Y, Z) = (1, 1, 0), (1, 8, 1)$ . Set  $K = \mathbb{Q}(\theta)$ ,  $\theta^3 + 3\theta + 1 = 0$ . The ring of integers is  $\mathbb{Z}[\theta]$ ; a fundamental unit is  $\epsilon = \theta$ ; and the class number is 1. We have factorizations into prime ideals as follows:

$$(2), (3) = p_3^3, (5) = p_5^2 p'_5,$$

with  $p_3 = (2 + \theta^2)$ ,  $p_5 = (1 + \theta^2)$ ,  $p'_5 = (4 + \theta^2)$ . The equation becomes

$$\text{Norm}_{K/\mathbb{Q}}(X^2 - (4\theta + 1)Z^2) = Y^2,$$

equivalently,

$$(X^2 - (4\theta + 1)Z^2)(X^2 + (-2\theta^2 - 4)XZ + (2\theta^2 + 7)Z^2)(X^2 + (2\theta^2 + 4)XZ + (2\theta^2 + 7)Z^2) = Y^2.$$

The gcd  $(X^2 - (4\theta + 1)Z^2, X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4)$  divides  $2^4 p_3^3 p_5$ . So

$$(X^2 - (4\theta + 1)Z^2) = 2^i p_3^j p_5^k \square, \quad i, j, k = 0, 1;$$

and taking norms,  $2^{3i} 3^j 5^k = \square$ : so  $i = j = k = 0$ . Hence

$$X^2 - (4\theta + 1)Z^2 = \pm \epsilon^{-a} y_1^2, \quad X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4 = \pm \epsilon^a y_2^2,$$

for  $a = 0, -1$ , and  $y_1, y_2$  integers in  $K$  with  $y_1 y_2 = y$ .

Case of  $+$  sign,  $a = -1$ :

$$X^2 - (4\theta + 1)Z^2 = \epsilon y_1^2, \quad X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4 = \epsilon^{-1} y_2^2,$$

and the latter is not locally solvable at  $p_3$ .

Case of  $-$  sign,  $a = 0$ :

$$X^2 - (4\theta + 1)Z^2 = -y_1^2, \quad X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4 = -y_2^2,$$

and the latter is not locally solvable at  $p_3$ .

Case of  $+$  sign,  $a = 0$ :

$$X^2 - (4\theta + 1)Z^2 = y_1^2, \quad X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4 = y_2^2,$$

and the latter is an elliptic curve of rank 1 over  $\mathbb{Q}(\theta)$ . The rank is smaller than  $[K : \mathbb{Q}]$ , and the elliptic Chabauty routines in Magma [1] work effectively to show that the curve has precisely one point with  $X : Z$  rational, namely  $(X, Z) = (1, 0)$ , with  $(y_1, y_2) = (1, 1)$ . This leads to  $A = 0$ .

Case of  $-$  sign,  $a = -1$ :

$$X^2 - (4\theta + 1)Z^2 = -\epsilon y_1^2, \quad X^4 + (4\theta - 2)X^2Z^2 + (16\theta^2 - 4\theta + 49)Z^4 = -\epsilon^{-1} y_2^2,$$

and the latter is an elliptic curve of rank 1 over  $\mathbb{Q}(\theta)$ . As above, elliptic Chabauty techniques show there is precisely one pair of points with  $X : Z$  rational, namely  $(X, \pm Z) = (1, 1)$ , with  $(y_1, y_2) = (2, 4)$ . These points pull back to  $A = 0$ .  $\square$

### Theorem 4.3.

(1) *There are no trinomials  $x^6 + Ax^2 + B$  with reducibility type  $(1, 2, 3)$ .*

(2) If  $x^6 + Ax^2 + B$  has reducibility type  $(2, 2, 2)$  then either

$$(A, B) = (-s^2 - sv - v^2, -sv(s + v)), \quad s, v \in \mathbb{Q}, \quad sv(s + v) \neq 0,$$

with

$$x^6 + Ax^2 + B = (x^2 + s)(x^2 + v)(x^2 - s - v);$$

or, up to scaling,

$$(A, B) = (-(v - 1)(3v - 1), -v^2(2v - 1)), \quad v \in \mathbb{Q}, \quad v \neq 0, 1, 1/2, 1/3.$$

with

$$x^6 + Ax^2 + B = (x^2 + x + v)(x^2 - x + v)(x^2 - 2v + 1).$$

*Proof.* The first part of the Theorem is a simple consequence of the fact that if  $f(u) = 0$  for some  $u \in \mathbb{Q} \setminus \{0\}$  then  $f(-u) = 0$  and thus we have two rational roots. In order to prove the second part of the Theorem, suppose

$$x^6 + Ax^2 + B = (x^2 + px + q)(x^2 + rx + s)(x^2 + ux + v).$$

Equating coefficients of  $x^5, x^4, x^3, x$ :

$$-p - r - u = 0, \quad -p(u + r) - q - ur - s - v = 0,$$

$$-(s + ru + v)p - (r + u)q - vr - us = 0, \quad -qsu - qrv - psv = 0.$$

Eliminating  $p, q, s$ :

$$ru(r + u)(r^4 + 2r^3u + 3r^2u^2 + 2ru^3 + 2u^4 - 2r^2v - 2ruv - 8u^2v + 9v^2) = 0.$$

The latter factor has discriminant in  $v$  equal to  $-8(2r + u)^2(r^2 + ru + u^2)$ , which is a perfect square if and only if  $2r + u = 0$ , leading to  $p = r = u = 0$ ,  $q = -s - v$ , and  $(A, B) = (-s^2 - sv - v^2, -sv(s + v))$ . If instead  $ru = 0$ , then symmetry allows us to take without loss of generality  $r = 0$ . Then  $p = -u$ ,  $q = -s + u^2 - v$ , and  $u(s - u^2 + 2v) = 0$ . The case  $u = 0$  results in the previous factorization; and the case  $s = u^2 - 2v$  results in  $(A, B) = (-(u^2 - v)(u^2 - 3v), v^2(u^2 - 2v))$ , which on scaling so that  $u = 1$ , gives the assertion in the Theorem. Finally, the case  $r = -u$  leads to the same factorization.  $\square$

#### Theorem 4.4.

(1) If  $x^6 + Ax^3 + B$  has reducibility type  $(2, 2, 2)$  then up to scaling

$$A = -27u(u + 1), \quad B = 27(u^2 + u + 1)^3, \quad u \neq 0, -1, -1/2,$$

with

$$x^6 - 27u(u + 1)x^3 + 27(u^2 + u + 1)^3 = (x^2 + 3x + 3(u^2 + u + 1))(x^2 - 3(u + 1)x + 3(u^2 + u + 1))(x^2 + 3ux + 3(u^2 + u + 1)).$$

(2) If  $x^6 + Ax^3 + B$  has reducibility type  $(1, 1, 2, 2)$  then up to scaling

$$A = -u^3 - 1, \quad B = u^3, \quad u \neq 0, -1$$

and

$$x^6 + Ax^3 + B = (x - 1)(x - u)(x^2 + x + 1)(x^2 + ux + u^2).$$

(3) There are no trinomials  $x^6 + Ax^3 + B$  with reducibility type  $(1, 1, 1, 1, 2)$ .

(4) If  $x^6 + Ax^3 + B$  has reducibility type  $(1, 2, 3)$ , then up to scaling,  $(A, B) = (t - 1, -t)$ , where  $t$  is not a cube, and

$$x^6 + (t - 1)x^3 - t = (x - 1)(x^2 + x + 1)(x^3 + t).$$

*Proof.* To prove the first two parts of the Theorem, suppose that  $x^6 + Ax^3 + B = (x^2 + px + q)(x^2 + rx + s)(x^2 + ux + v)$  and equate coefficients of  $x^5, x^4, x^2, x$ :

$$\begin{aligned} p + r + u &= 0, & p(u + r) + q + ur + s + v &= 0, \\ qs + qru + psu + qv + prv + sv &= 0, & qsu + qrv + psv &= 0. \end{aligned}$$

Eliminating  $r, s, v$ :

$$(p^2 - q)(p^2 + pu + u^2)(p^2 - 3q + pu + u^2)(q + pu + u^2) = 0.$$

There are three cases:

- (1) If  $q = p^2$ , then either  $v = u^2$  and on scaling so that  $p = 1$ , we have the factorization in statement (2) of the Theorem; or  $v = -p^2 - pu$ , which leads to the same factorization under change of variable.
- (2) If  $q = \frac{1}{3}(p^2 + pu + u^2)$  then either  $v = \frac{1}{3}(p^2 + pu + u^2)$  and on scaling to  $p = 3$ , we have the factorization in statement (1) of the Theorem; or  $v = -\frac{2}{3}p^2 - \frac{5}{3}pu + \frac{1}{3}u^2$ ,  $p \in \{0, u, -1/2u, -2u\}$ , with corresponding factorizations that either have  $A = 0$  or are special cases of the factorization in case (1).
- (3) If  $q = -pu - u^2$  then  $v = u^2$  and again we have a symmetry of the factorization in case (1).

The third part of the Theorem is immediate from the second part.

Finally, suppose  $x^6 + Ax^3 + B = (x - u)(x^2 + px + q)(x^3 + rx^2 + sx + t)$ , and equate coefficients:

$$\begin{aligned} p + r - u &= 0, & q + pr + s - pu - ru &= 0, \\ -A + qr + ps + t - qu - pru - su &= 0, & qs + pt - qru - psu - tu, \\ qt - qsu - ptu &= 0, & -B - qtu &= 0. \end{aligned}$$

If  $r = 0$ , it follows that  $p = u$ ,  $s = 0$ ,  $q = u^2$ , and we derive the factorization in the statement (4) of the Theorem. If  $r \neq 0$ , then eliminating  $p, q, t$ ,

$$(-s + ru)(r^4 - 2r^2s + s^2 - r^3u + rsu + r^2u^2) = 0,$$

and the latter factor has discriminant in  $u$  equal to  $-3r^2(r^2 - s)^2$ , which is a perfect square if and only if  $r^2 - s = 0$ . This leads to  $B = 0$ . And if  $s = ru$ , then  $(A, B) = ((r - 2u)(r^2 - ru + u^2), -(r - u)^3u^3)$ , and the factorization is again of type (1, 1, 2, 2).  $\square$

## 5. REDUCIBILITY TYPE OF SOME HIGHER DEGREE TRINOMIALS

**Theorem 5.1.** *If  $x^7 + Ax + B$  has reducibility type (1, 2, 4) then*

$$\begin{aligned} A &= w^3 - v(3v + 1)w^2 + v(v^3 + 3v^2 - 2v + 1)w - v(v^4 - v^3 + v^2 - v + 1), \\ B &= -w(w^2 - (3v^2 - 2v + 1)w + (v^4 - v^3 + v^2 - v + 1)) \end{aligned}$$

and

$$4v^6 - 8v^5 + 9v^4 - 4v^3 - 6v^2 + 12v - 3 = \square = (4v^3 - 3v^2 + 2v - 1 - 2(3v - 1)w)^2$$

for some  $v \in \mathbb{Q}$ .

*Proof.* We suppose  $x^7 + Ax + B = (x - 1)(x^2 + vx + w)(x^4 + px^3 + qx^2 + rx + s)$ , and equate coefficients:

$$\begin{aligned} p + v - 1 &= 0, & -q + p - pv + v - w &= 0, \\ -r + q - qv + pv - pw + w &= 0, & -s + r - rv + qv - qw + pw &= 0, \\ s - sv + rv - rw + qw &= 0, & A + sv - sw + rw &= 0, & B + sw &= 0. \end{aligned}$$

Eliminating  $p, q, r, s$ ,

$$A = w^3 - v(3v + 1)w^2 + v(v^3 + 3v^2 - 2v + 1)w - v(v^4 - v^3 + v^2 - v + 1),$$

$$B = -w(w^2 - (3v^2 - 2v + 1)w + (v^4 - v^3 + v^2 - v + 1)),$$

with

$$4v^6 - 8v^5 + 9v^4 - 4v^3 - 6v^2 + 12v - 3 = (4v^3 - 3v^2 + 2v - 1 - 2(3v - 1)w)^2.$$

□

We have been unable to determine the finitely many rational points on the curve  $C$  of genus 2:

$$C : y^2 = 4v^6 - 8v^5 + 9v^4 - 4v^3 - 6v^2 + 12v - 3.$$

but believe the set of (finite) points is the following:

$$(v, \pm y) = (1, 2), \quad (-1, 2), \quad (1/3, 14/27), \quad (7/5, 446/125),$$

with corresponding  $w = 0, 1$ ;  $w = 1, 3/2$ ;  $w = 13/9$ ; and  $w = 13/25, 327/200$ , respectively. The first leads to  $B = 0$ ; and after scaling, the others determine the following factorizations, which we believe to be the complete list of the given type:

$$x^7 - 232x + 336 = (x - 2)(x^2 - 2x + 6)(x^4 + 4x^3 + 6x^2 - 4x - 28),$$

$$x^7 + 1247x - 5928 = (x - 3)(x^2 + x + 13)(x^4 + 2x^3 - 6x^2 + 7x + 152),$$

$$x^7 - 9073x - 32760 = (x - 5)(x^2 + 7x + 13)(x^4 - 2x^3 + 26x^2 - 31x + 504),$$

$$x^7 - 204214984x + 2804299680 = (x - 20)(x^2 + 28x + 654)(x^4 - 8x^3 - 30x^2 + 14072x - 214396).$$

**Remark 5.2.** It is interesting to note that to the best of our knowledge, these trinomials with reducibility type  $(1, 2, 4)$  give the first explicit examples showing that some (exceptional) finite sets defined in Theorems 3 of Schinzel [4, 5] are non-empty.

**Theorem 5.3.** (1) *If  $x^7 + Ax + B$  has reducibility type  $(3, 4)$  then up to scaling*

$$(A, B) = ((4u^2 - 5u + 2)(u^3 - u^2 - 2u + 1)/(2u - 3)^2,$$

$$(3u - 1)(2u - 1)(u - 1)(u^2 - u + 1)/(2u - 3)^2), \quad u \neq 1, \frac{1}{2}, \frac{1}{3}, \frac{3}{2},$$

with

$$x^7 + Ax + B = \left( x^3 + x^2 + ux + \frac{(3u - 1)(u - 1)}{2u - 3} \right) \left( x^4 - x^3 - (u - 1)x^2 + \frac{(u^2 - 4u + 2)}{2u - 3}x + \frac{(2u - 1)(u^2 - u + 1)}{2u - 3} \right).$$

(2) *There are no trinomials  $x^7 + Ax^2 + B$  with reducibility type  $(3, 4)$ .*

(3) *If  $x^7 + Ax^3 + B$  has reducibility type  $(3, 4)$  then up to scaling  $(A, B) = (2, -1)$  with*

$$x^7 + Ax^3 + B = (x^3 + x^2 - 1)(x^4 - x^3 + x^2 + 1).$$

*Proof.* The first part is immediate on comparing coefficients in the expression  $x^7 + Ax + B = (x^4 + px^3 + qx^2 + rx + s)(x^3 + tx^2 + ux + v)$ , and scaling so that  $t = 1$  (in fact this result can be found in [3]). For the second part, suppose



$x^7 + Ax^2 + B = (x^4 + px^3 + qx^2 + rx + s)(x^3 + tx^2 + ux + v)$ . Comparing coefficients and eliminating  $p, q, r, s$ :

$$4u^3 + 4t^2u^2 - 4t^4u + t^6 = (t^3 - 4tu + 2v)^2,$$

the equation of an elliptic curve with rank 0 and torsion group of order 3. The torsion leads to the  $(1, 3, 3)$  factorization  $x^7 - 2x^2 + 1 = (x-1)(x^3+x+1)(x^3+x^2-1)$ . For the third part, suppose  $x^7 + Ax^3 + B = (x^4 + px^3 + qx^2 + rx + s)(x^3 + tx^2 + ux + v)$ . Comparing coefficients and eliminating  $p, q, r, s$ :

$$(u - t^2)(2u - t^2)(2u^2 + t^2u + t^4) = (2tv - t^2u - 2u^2 + t^4)^2,$$

the equation of an elliptic curve of rank 0 and torsion group of order 6. The only non-trivial trinomial that results is the one in the statement of the Theorem.  $\square$

**Theorem 5.4.** *The trinomial  $x^8 + Ax^3 + B$  is divisible by the polynomial  $x^3 + ux^2 + vx + w$  if and only if either  $u = 0$  and  $(A, B) = (-3t^5, -t^8)$ ,  $t \in \mathbb{Q} \setminus \{0\}$ , with (upon scaling)*

$$x^8 - 3x^3 - 1 = (x^3 + x + 1)(x^5 - x^3 - x^2 + x - 1);$$

or, upon scaling to  $u = 1$ ,

$$(2) \quad A = 1 - 5v + 6v^2 - v^3 + 4w - 6vw + w^2,$$

$$(3) \quad B = -w(v - 3v^2 + v^3 - w + 4vw - w^2),$$

and

$$(4) \quad (v^2 + 2v - 1)(4v^3 - 3v^2 + 2v - 1) = \square = (2(v + 2)w - (3v - 1)(v + 1))^2.$$

In particular the only trinomials  $x^8 + Ax^3 + B$  with reducibility type (3, 5) are those with the numbers (1), (2), (3), (4) on the list at the end of Schinzel [3].

*Proof.* Applying the Division Algorithm, the remainder on dividing  $x^8 + Ax^3 + B$  by  $x^3 + ux^2 + vx + w$  is equal to  $ax^2 + bx + c$ , with

$$a = -Au + u^6 - 5u^4v + 6u^2v^2 - v^3 + 4u^3w - 6uvw + w^2,$$

$$b = -Av + u^5v - 4u^3v^2 + 3uv^3 - u^4w + 6u^2vw - 3v^2w - 2uw^2,$$

$$c = B - Aw + u^5w - 4u^3vw + 3uv^2w + 3u^2w^2 - 2vw^2.$$

If  $u = 0$ , then it follows that  $(v, w) = (t^2, t^3)$ ,  $(A, B) = (-3t^5, -t^8)$ , for some non-zero  $t \in \mathbb{Q}$ . If  $u \neq 0$ , then setting  $a = c = 0$  gives (2), (3); and demanding  $b = 0$  gives (4) in the form

$$(v^2 + 2u^2v - u^4)(4v^3 - 3u^2v^2 + 2u^4v - u^6) = (2(v + 2u^2)w - u(3v - u^2)(v + u^2))^2.$$

The problem of determining all trinomials  $x^8 + ax^3 + b$  with reducibility type (3, 5) is thus reduced to finding all rational points on the genus two curve

$$C : (v^2 + 2u^2v - u^4)(4v^3 - 3u^2v^2 + 2u^4v - u^6) = \square,$$

where we can assume without loss of generality that  $(v, u^2) = 1$ . We show the points comprise precisely the following set:  $(v, u^2) = (1, 0), (0, 1), (1, 1), (-2, 1)$ , which lead just to the factorizations on the Schinzel list.

Observe first that  $r = v/u^2$  satisfies  $(r^2 + 2r - 1)(4r^3 - 3r^2 + 2r - 1) > 0$ , so necessarily

$$(5) \quad (-1 - \sqrt{2}) < u/v^2 < (-1 + \sqrt{2}), \text{ or } 0.60583 < u/v^2.$$

Factoring over  $\mathbb{Z}$ ,

$$(6) \quad v^2 + 2u^2v - u^4 = c_0g^2, \quad 4v^3 - 3u^2v^2 + 2u^4v - u^6 = c_0h^2,$$

with  $c_0 = \pm 1, \pm 2$ , and  $g, h \in \mathbb{Z}$ . When  $c_0 = 1, -2$ , the latter elliptic curve has rank 0, and leads only to  $u = 0$ ; so we need only consider  $c_0 = -1, 2$ .

We need to work over two number fields. First,  $K = \mathbb{Q}(\sqrt{2})$  with integer ring  $\mathbb{Z}[\sqrt{2}]$ , class number 1, and fundamental unit  $e = 1 + \sqrt{2}$ . Second,  $L = \mathbb{Q}(\theta)$ , where  $\theta^3 - 2\theta^2 + 3\theta - 4 = 0$ . The ring of integers is  $\mathbb{Z}[\theta]$ ; the class number is 1; and a fundamental unit is  $\epsilon = -1 - \theta + \theta^2$ , of norm 1. There are factorizations into prime ideals as follows:

$$(2) = p_{21}p_{22}^2 = (2 - \theta)(-1 + \theta)^2, \quad (5) = p_5^3 = (3 - \theta + \theta^2)^2.$$

Case I:  $c_0 = 2$ .

Factoring over  $L$  the second equation at (6),

$$(\theta v - u^2)((\theta^2 - 2\theta + 3)v^2 + (\theta - 2)vu^2 + u^4) = 2h^2$$

and the (ideal) gcd of the factors on the left divides  $(3 - 4\theta + 3\theta^2) = p_{22}^3p_5^2$ . Thus

$$\theta v - u^2 = \pm \epsilon^i p_{22}^j p_5^k \rho^2,$$

for  $i, j, k = 0, 1$ , and  $\rho \in \mathbb{Z}[\theta]$ . Taking norms

$$\pm 2^j 5^k = 2\Box,$$

forcing the plus sign, and  $(j, k) = (1, 0)$ . Hence

$$\theta v - u^2 = \epsilon^i (-1 + \theta) \rho^2, \quad i = 0, 1.$$

When  $i = 0$ , we have

$$\theta v - u^2 = (-1 + \theta) \rho^2, \quad v^2 + 2vu^2 - u^4 = 2g^2,$$

so that

$$(\theta v - u^2)(v^2 + 2vu^2 - u^4) = 2(-1 + \theta)\Box,$$

the equation of an elliptic curve of rank 1 over  $\mathbb{Q}(\theta)$ . The elliptic Chabauty routines in Magma show that the only points with  $u : v$  rational are  $(v, \pm u) = (1, 0), (1, 1)$ .

When  $i = 1$ ,

$$\theta v - u^2 = \epsilon(-1 + \theta) \rho^2, \quad v^2 + 2vu^2 - u^4 = 2g^2,$$

so that

$$(\theta v - u^2)(v^2 + 2vu^2 - u^4) = 2\epsilon(-1 + \theta)\Box.$$

again, an elliptic curve of rank 1 over  $\mathbb{Q}(\theta)$ . The only points with  $u : v$  rational are given by  $(v, \pm u) = (1, 0)$ .

Case II:  $c_0 = -1$ :

Factoring over  $K$  the first equation at (6),

$$(v + (1 + \sqrt{2})u^2)(v + (1 - \sqrt{2})u^2) = -g^2,$$

and the great common divisor of the two factors on the left divides  $2\sqrt{2}$ . Thus

$$v + (1 + \sqrt{2})u^2 = \pm e^i (\sqrt{2})^j \alpha^2,$$

for  $i, j = 0, 1$ , and  $\alpha \in \mathbb{Z}[\sqrt{2}]$ . From (5), we must have the plus sign. Taking norms,

$$(-1)^{i+j} 2^j = -\Box,$$

forcing  $(i, j) = (1, 0)$ . Thus

$$v + (1 + \sqrt{2})u^2 = e\alpha^2.$$

As above, on factoring over  $L$  the second equation at (6),

$$\theta v - u^2 = \pm \epsilon^i p_{22}^j p_5^k \rho^2,$$

where  $i, j, k = 0, 1$ , and  $\rho \in \mathbb{Z}[\theta]$ . Taking norms,

$$\pm 2^j 5^k = -\square,$$

forcing the minus sign, and  $(j, k) = (0, 0)$ . Hence

$$\theta v - u^2 = -\epsilon^i \rho^2, \quad (\theta^2 - 2\theta + 3)v^2 + (\theta - 2)vu^2 + u^4 = \epsilon^{-i} \sigma^2,$$

for  $i = 0, 1$ , and  $\sigma \in \mathbb{Z}[\theta]$ .

In the case  $i = 1$ , then

$$\theta v - u^2 = -\epsilon \rho^2, \quad v^2 + 2vu^2 - u^4 = -g^2.$$

Thus

$$(\theta v - u^2)(v^2 + 2vu^2 - u^4) = \epsilon \square,$$

and Magma tells us this curve has rank 0 over  $L$ ; the only points are the torsion points given by  $v/u^2 = 1/\theta$ .

Suppose finally  $i = 0$ . Trying to work exclusively over the quadratic or the cubic number field led to problems with the computation. Instead, consider

$$((\theta^2 - 2\theta + 3)v^2 + (\theta - 2)vu^2 + u^4)(v + (1 + \sqrt{2})u^2) = e\square,$$

the equation of an elliptic curve over the compositum of  $K$  and  $L$ . The rank is determined to be 2, and the elliptic Chabauty routines show that the only points with  $v : u$  rational are given by  $(v, u^2) = (1, 0), (0, 1), (-2, 1)$ .  $\square$

**Theorem 5.5.** *The trinomial  $x^9 + Ax^2 + B$  is divisible by the polynomial  $x^3 + ux^2 + vx + w$  if and only if*

$$A = u^7 - 6u^5v + 10u^3v^2 - 4uv^3 + 5u^4w - 12u^2vw + 3v^2w + 3uw^2,$$

$$B = w(u^6 - 5u^4v + 6u^2v^2 - v^3 + 4u^3w - 6uvw + w^2),$$

and

$$(7) \quad u^{10} - 4u^8v + 10u^6v^2 - 12u^4v^3 - 3u^2v^4 + 12v^5 = (6(u^2 - v)w + u^5 - 8u^3v + 9uv^2)^2.$$

*In particular the only trinomials  $x^9 + Ax^2 + B$  with reducibility type (3, 6) are those with the numbers (6), (7), (8) on the list in Schinzel [3], namely, up to scaling,*

$$x^9 \pm 32x^2 \mp 64, \quad x^9 \pm 81x^2 \mp 54, \quad x^9 \pm 729x^2 \mp 1458.$$

*Proof.* The Division Algorithm is used as in the preceding Theorem to obtain the first statement. To complete the proof, we need to determine all rational points on the curve (7) of genus 2. Take the equation in the form

$$X^5 - 3X^4z^2 - 144X^3z^4 + 1440X^2z^6 - 6912Xz^8 + 20736z^{10} = Y^2,$$

where  $X = 12vz^2/u^2$ . Set  $K = \mathbb{Q}(\theta)$ ,  $\theta^5 + \theta^4 + 4\theta^3 + 4\theta^2 - 8\theta + 4 = 0$ , so that

$$\text{Norm}_{K/\mathbb{Q}}(X + (\theta^4 + 4\theta^2 - 8)z^2) = Y^2.$$

The ring of integers in  $K$  has basis  $\{1, \theta, \theta^2, 1/2(\theta^3 + \theta^2), 1/2(\theta^4 + \theta^2)\}$ . There are ideal factorizations:

$$(2) = p_{21}p_{22}^4, \quad (3) = p_{31}^3p_{32}^2, \quad (7) = p_{71}^3p_{72}^2;$$

and fundamental units are given by

$$\epsilon_1 = [2, -5, 4, -1, 2], \quad \epsilon_2 = [0, -11, 47, -20, -29].$$

We have

$$(X + (\theta^4 + 4\theta^2 - 8)z^2) = p_{22}^{i_1} p_{31}^{j_1} p_{32}^{j_2} p_{71}^{k_1} p_{72}^{k_2} \square, \quad i_1, j_1, j_2, k_1, k_2 = 0, 1;$$

and on taking norms,

$$2^{i_1} 3^{j_1+j_2} 7^{k_1+k_2} = \square,$$

so that  $i_1 = 0, j_1 = j_2, k_1 = k_2$ . If  $k_1 = k_2 = 1$ , then  $X + 4z^2 \equiv 0 \pmod{7}$  and  $X + 3z^2 \equiv 0 \pmod{7}$ , impossible. If  $j_1 = j_2 = 1$ , then  $3 \mid X$ , and  $(\theta^4 + 4\theta^2 - 8)z^2 \equiv 0 \pmod{p_{31}^3}$ , contradiction. Thus

$$(X + (\theta^4 + 4\theta^2 - 8)z^2) = \square,$$

so that with  $\delta = \pm \epsilon_1^{l_1} \epsilon_2^{l_2}$ ,  $l_1, l_2 = 0, 1$ ,

$$\begin{aligned} X + (\theta^4 + 4\theta^2 - 8)z^2 &= \delta^{-1} a^2, \\ X^4 - (\theta^4 + 4\theta^2 - 5)X^3 z^2 - 12(\theta^3 - \theta^2 + 5\theta + 7)X^2 z^4 \\ &\quad - 144(\theta^2 - 2\theta - 3)Xz^6 - 1728(\theta + 1)z^8 = \delta b^2, \end{aligned}$$

for integers  $a, b$  of  $K$  satisfying  $ab = y$ . Eliminating  $X$  results in an eighth degree equation homogeneous in  $a, z$ , that is everywhere locally solvable for precisely the values  $\delta = 1, -\epsilon_1 \epsilon_2$ .

Case I:  $\delta = 1$ .

$$\begin{aligned} X^4 + (-\theta^4 - 4\theta^2 + 5)X^3 z^2 - 12(\theta^3 - \theta^2 + 5\theta + 7)X^2 z^4 \\ - 144(\theta^2 - 2\theta - 3)Xz^6 - 1728(\theta + 1)z^8 = b^2. \end{aligned}$$

The curve is birationally equivalent to

$$\begin{aligned} E : y^2 = x^3 - (\theta^4 + 3\theta^3 + 6\theta^2 + 14\theta + 6)x^2 + \frac{1}{3}(6\theta^4 + 19\theta^3 + 47\theta^2 + 92\theta + 94)x \\ + \frac{1}{9}(851\theta^4 + 1318\theta^3 + 4040\theta^2 + 5409\theta - 4448), \end{aligned}$$

of rank 4 over  $K$ . Generators for a subgroup of odd index in  $E(K)/2E(K)$  are given by

$$\begin{aligned} &(0, \frac{1}{6}(17\theta^4 + 32\theta^3 + 95\theta^2 + 150\theta - 18)); \\ &(\frac{1}{3}(-\theta^4 - 2\theta^3 - 8\theta^2 - 10\theta), \frac{1}{2}(-3\theta^4 - 6\theta^3 - 17\theta^2 - 26\theta + 6)); \\ &(\frac{1}{2}(3\theta^4 + 7\theta^3 + 18\theta^2 + 26\theta), \frac{1}{6}(\theta^4 + 10\theta^3 + 37\theta^2 + 42\theta + 30)); \\ &(\frac{1}{3}(-\theta^4 + \theta^3 - 2\theta^2 + 8\theta + 24), \frac{1}{2}(3\theta^4 + 4\theta^3 + 13\theta^2 + 14\theta - 22)), \end{aligned}$$

and the Magma routines succeed in showing the only valid solutions are  $(X, z^2) = (1, 0), (12, 1)$ . (We list the generators above because the initial machine computation returned a subgroup of index 3, and the routines failed).

Case II:  $\delta = -\epsilon_1 \epsilon_2$ .

$$\begin{aligned} X^4 + (-\theta^4 - 4\theta^2 + 5)X^3 z^2 - 12(\theta^3 - \theta^2 + 5\theta + 7)X^2 z^4 \\ - 144(\theta^2 - 2\theta - 3)Xz^6 - 1728(\theta + 1)z^8 = -\epsilon_1 \epsilon_2 b^2. \end{aligned}$$

The point  $(0, -48\theta^4 - 228\theta^3 - 60\theta^2 + 264\theta - 144)$  leads to birational equivalence with the curve

$$y^2 = x^3 + (3\theta^3 + \theta^2 + 4\theta + 1)x^2 - (6\theta^4 + 6\theta^3 - 20\theta^2 + 28\theta - 35)x - (18\theta^4 + 45\theta^3 + 53\theta^2 - 100\theta - 71)$$

of rank 3 over  $K$ , and the Magma routines are successful in showing that the only valid solutions arise for  $(X, z^2) = (0, 1)$ .  $\square$

Similarly we can obtain the following.

**Theorem 5.6.** *The trinomial  $x^{10} + Ax + B$  is divisible by the polynomial  $x^3 + ux^2 + vx + w$  if and only if*

$$A = (w - uv)(u^6 - 6u^4v + 10u^2v^2 - 4v^3 + 4u^3w - 8uvw + w^2),$$

$$B = -w(u^7 - 6u^5v + 10u^3v^2 - 4uv^3 + 5u^4w - 12u^2vw + 3v^2w + 3uw^2),$$

and

$$(8) \quad 3u^{10} - 15u^8v + 25u^6v^2 - 15u^4v^3 + 3v^5 = (3(2u^2 - v)w + 3u^5 - 10u^3v + 6uv^2)^2$$

**Remark 5.7.** Unfortunately, we are unable to determine all rational points on the curve (8) of genus two. The rational points  $(u, \pm v, w)$  with height at most  $10^6$  (with  $w \neq 0$ ), and their corresponding trinomials up to scaling, are as follows:

$$\begin{aligned} (0, 3, 3), & \quad x^{10} \pm 297x - 243, \\ (1, 1, \frac{2}{3}), & \quad x^{10} \pm 8019x + 13122, \\ (1, 2, \frac{17}{14}), & \quad x^{10} \pm 261312546880x + 2485545010816. \end{aligned}$$

The first example is (11) on the list in Schinzel [3]. The second and third examples, discovered by Cislowska, are listed as (11a), (12a) in the reprinting of Schinzel [3] in Schinzel [6]. It is likely they are the only such.

## 6. TRINOMIALS WITH FORCED FACTORS

For certain trinomials where  $(m, n) > 1$  we can force an algebraic factor and determine the reducibility type of the quotient.

**Theorem 6.1.** *Suppose that  $x^4 + Ax + B$  has the rational non-zero root  $v$ . Then reducibility of  $(x^8 + Ax^2 + B)/(x^2 - v)$  implies reducibility type  $(3, 3)$ , occurring precisely when (up to scaling)*

$$(9) \quad A = -\frac{(q^2 + 2q - 1)(9q^2 - 10q + 3)}{4}, \quad B = \frac{(q - 1)^2(2q - 1)(3q - 1)^2}{4}, \quad q \neq 1, \frac{1}{2}, \frac{1}{3}.$$

*Proof.* By Lemma 29 of Schinzel [3], if  $(x^8 + Ax^2 + B)/(x^2 - v) = x^6 + vx^4 + v^2x^2 + v^3 + A$  is reducible, then it takes the form  $(x^3 + px^2 + qx + r)(x^3 - px^2 + qx - r)$ . Comparing coefficients of powers of  $x$  and eliminating  $r$  gives  $(A, B)$  as in the Theorem after scaling so that  $p = 1$  (it is easy to check that  $p = 0$  results in  $v = 0$ ). Further, the cubic factor  $x^3 + x^2 + qx - \frac{(q-1)(3q-1)}{2}$  is irreducible. For if  $u$  is a rational root, then  $6u^3 + 7u^2 + 4u + 1 = (3q - u - 2)^2$ . But the corresponding elliptic curve has rank 0, and the only finite points occur at  $u = 0, -1/2$ , giving  $B = 0$ .  $\square$

**Theorem 6.2.** *Suppose  $x^5 + Ax + B$  has the quadratic factor  $x^2 + ux + v$ . Then the polynomial  $(x^{10} + Ax^2 + B)/(x^4 + ux^2 + v)$  has reducibility type  $(3, 3)$  infinitely often, parameterized by the elliptic curve  $Y^2 = X(X^2 + 12X - 4)$  of rank 1.*

*Proof.* The divisibility condition of the Theorem is that

$$(A, B) = (-u^4 + 3u^2v - v^2, -uv(u^2 - 2v)),$$

and then

$$(x^{10} + Ax^2 + B)/(x^4 + ux^2 + v) = x^6 - ux^4 + (u^2 - v)x^2 + u(2v - u^2).$$

The sextic can only split in the form

$$x^6 - ux^4 + (u^2 - v)x^2 + u(2v - u^2) = (x^3 + px^2 + qx + r)(x^3 - px^2 + qx - r),$$

and comparing coefficients,  $u = p^2 - 2q$ ,  $v = p^4 - 4p^2q + 3q^2 + 2pr$ , and

$$(2q - p^2)(2q^2 + 4p^2q - 3p^4) = (r + 2p(p^2 - 2q))^2.$$

The latter is the equation of an elliptic curve with model  $Y^2 = X(X^2 + 12X - 4)$ , having rank 1, and generator  $P(X, Y) = (5, 3)$ . Each multiple of  $P$  pulls back to a factorization of the sextic into two cubics. For the cubics to be reducible,  $x^3 + px^2 + qx + r$  will have rational root  $w$  say, and necessarily

$$(2q - p^2)(2q^2 + 4p^2q - 3p^4) = (-w^3 - pw^2 - qw + 2p(p^2 - 2q))^2.$$

This latter is the equation of a curve of genus 4, with only finitely many points (likely just  $(p, q, w) = (\pm 2, 2, 0), (2, 3, -1), (-2, 3, 1)$ ).

Examples:  $(p, q, r) = (2, 3, 2)$  gives  $(u, v) = (-2, 3)$ ,  $(A, B) = (11, -12)$  and

$$x^{10} + 11x^2 - 12 = (x + 1)(x - 1)(x^2 + x + 2)(x^2 - x + 2)(3 - 2x^2 + x^4).$$

And  $(p, q, r) = (2, 3, 14)$ ,  $(u, v) = (-2, 51)$ ,  $(A, B) = (-2005, -9996)$  with

$$x^{10} - 2005x^2 - 9996 = (x^3 - 2x^2 + 3x - 14)(x^3 + 2x^2 + 3x + 14)(x^4 - 2x^2 + 51).$$

□

**Theorem 6.3.** *Suppose  $x^5 + Ax^2 + B$  has the quadratic factor  $x^2 + ux + v$ . Then the polynomial  $(x^{10} + Ax^4 + B)/(x^4 + ux^2 + v)$  is reducible (with type  $(3, 3)$ ) in precisely the following four cases (up to scaling):*

- $x^{10} + 6875x^4 - 312500 = (x^3 - 5x^2 + 50)(x^3 + 5x^2 - 50)(x^4 + 25x^2 + 125)$ ;
- $x^{10} + 891x^4 - 34992 = (x^3 - 3x^2 + 9x - 18)(x^3 + 3x^2 + 9x + 18)(x^4 - 9x^2 + 108)$ ;
- $x^{10} - 119527785x^4 - 2195696106864 =$   
 $(x^3 + 39x^2 + 507x + 3042)(x^3 - 39x^2 + 507x - 3042)(x^4 + 507x^2 + 237276)$ ;
- $x^{10} + 37347689456x^4 - 609669805268160000 =$   
 $(x^3 + 28x^2 + 1960x + 191100)(x^3 - 28x^2 + 1960x - 191100)(x^4 - 3136x^2 + 16694496)$ .

*Proof.* By scaling, we may suppose that  $A, B, u, v$  are integers. Clearly  $u \neq 0$ , and the divisibility condition is that

$$A = \frac{u^4 - 3u^2v + v^2}{u}, \quad B = \frac{-v^2(u^2 - v)}{u},$$

in which case  $(x^{10} + Ax^4 + B)/(x^4 + ux^2 + v) = x^6 - ux^4 + (u^2 - v)x^2 - v(u^2 - v)/u$ . The sextic is reducible precisely when

$$x^6 - ux^4 + (u^2 - v)x^2 - v(u^2 - v)/u = (x^3 + px^2 + qx + r)(x^3 - px^2 + qx - r),$$

and comparing coefficients,

$$p^2 - 2q - u = 0, \quad -q^2 + 2pr + u^2 - v = 0, \quad r^2 - uv + v^2/u = 0.$$

Eliminating  $q, r$ :

$$(10) \quad 4p^2u(-p^4 + 4p^2u + u^2)(p^4 + 3u^2) = (4(4p^2 + u)v + u(p^4 - 10p^2u - 3u^2))^2,$$

equivalently,

$$(11) \quad U(U^2 + 3p^4)(U^2 + 12Up^2 - 9p^4) = V^2, \quad U = 3u,$$

where, without loss of generality,  $(U, p) = 1$ . This latter equation defines a curve of genus 2, and we show that its finite rational points are precisely

$$(12) \quad (U/p^2, \pm V) = (0, 0), (1, 4), (-3, 36), (3, 36), (-12, 126).$$

The first point corresponds to  $B = 0$ , and the remaining points return (up to scaling) the trinomials given in the Theorem.

We work in  $\mathbb{Q}(\sqrt{5})$ , with fundamental unit  $\epsilon = (1 + \sqrt{5})/2$ . Then

$$U(U^2 + 3p^4)(U + 3(2 + \sqrt{5})p^2)(U + 3(2 - \sqrt{5})p^2) = \square.$$

Now  $\gcd(U + 3(2 + \sqrt{5})p^2, U(U^2 + 3p^4)(U + 3(2 - \sqrt{5})p^2))$  divides  $2^4 3^3 \sqrt{5}$ . Thus we have:

$$U + 3(2 + \sqrt{5})p^2 = \gamma u^{-1} \square, \quad U(U^2 + 3p^4)(U + 3(2 - \sqrt{5})p^2) = \gamma u \square,$$

where the  $\gcd \gamma$  is a divisor of  $2^4 3^3 \sqrt{5}$  and  $u$  is a unit.

If  $\sqrt{5} \mid \gamma$ , then  $U \equiv -6p^2 \pmod{\sqrt{5}}$ , so  $U \equiv -p^2 \pmod{5}$ . It is not possible for both  $p, U$  to be divisible by 5; and thus  $5 \nmid U$ . However,  $U^2 + 12Up^2 - 9p^4 \equiv 0 \pmod{5}$ , so from (11), necessarily  $U^2 + 12Up^2 - 9p^4 \equiv 0 \pmod{25}$ . But  $(U + 6p^2)^2 - 45p^2 \equiv 0 \pmod{25}$  implies  $p \equiv 0 \equiv U \pmod{5}$ , contradiction.

Fix the square root of 5 to be positive. If  $\gamma u < 0$ , then  $U + 3(2 + \sqrt{5})p^2 = \gamma u^{-1} \square$  implies  $U < -3(2 + \sqrt{5})p^2 < 0$ ; but then

$$U < 0, \quad U^2 + 3p^4 > 0, \quad U + 3(2 - \sqrt{5})p^2 < -3(2 + \sqrt{5})p^2 + 3(2 - \sqrt{5})p^2 = -6\sqrt{5}p^2 < 0;$$

so the product of these three terms cannot be negative.

Accordingly,  $\gamma u$  takes one of the following values:  $2^i 3^j \epsilon^k$ , where, without loss of generality,  $i, j, k = 0, 1$ . Of the eight elliptic curves

$$U(U^2 + 3p^4)(U + 3(2 - \sqrt{5})p^2) = 2^i 3^j \epsilon^k \square$$

one has rank 0 (when  $(i, j, k) = (0, 0, 1)$ ), and the other seven have rank 1. The Magma routines run satisfactorily to show that the only solutions under the rationality constraint  $U/p^2 \in \mathbb{Q}$  are indeed those corresponding to the points at (12), together with the point at infinity.  $\square$

**Theorem 6.4.** *If  $x^4 + Ax + B$  has a rational root, say  $r$ , and the polynomial  $(x^{12} + Ax^3 + B)/(x^3 - r)$  has a cubic factor, then either*

$$(A, B) = (-(r - w)(r^2 + w^2), -rw(r^2 - rw + w^2)), \quad r, w \in \mathbb{Q}, \quad rw(r - w) \neq 0,$$

*with factorization*

$$x^{12} + Ax^3 + B = (x^3 - r)(x^3 + w)(x^6 + (r - w)x^3 + r^2 - rw + w^2);$$

*or, up to scaling,  $(A, B) = (128, 256), (-5616, -3888)$ , with*

- $x^{12} + 128x^3 + 256 = (x^3 + 4)(x^3 + 2x^2 + 4x + 4)(x^6 - 2x^5 + 8x^2 - 16x + 16)$ ,
- $x^{12} - 5616x^3 - 3888 = (x^3 - 18)(x^3 + 6x + 6)(x^6 - 6x^4 + 12x^3 + 36x^2 - 36x + 36)$ .

*Proof.* If  $x^4 + Ax + B$  has rational root  $r$ , then  $B = -Ar - r^4$ . Suppose that the polynomial  $(x^{12} + Ax^3 - Ar - r^4)/(x^3 - r)$  has a cubic factor. Then, say,

$$x^9 + rx^6 + r^2x^3 + r^3 + A = (x^3 + ux^2 + vx + w)(x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f),$$

Comparing coefficients, and eliminating  $a, b, c, d, e, f, w$ :

$$(13) \quad (3v^3 - 2r^2 + 3vru - 2ru^3 - 3vu^4 + u^6)(3v^6 - 9v^5u^2 + 2v^3ru^3 + 18v^4u^4 - 3v^2ru^5 - 21v^3u^6 + r^2u^6 + 3vru^7 + 15v^2u^8 - ru^9 - 6vu^{10} + u^{12}) = 0.$$

If the first factor at (13) is zero then

$$(4r - u(3v - 2u^2))^2 = 3(8v^3 + 3v^2u^2 - 12vu^4 + 4u^6),$$

the equation of an elliptic curve with minimal model  $y^2 + xy + y = x^3 - x^2 - 56x + 163$ . This curve has rank 0 and the torsion group is of order three. The torsion points lead to  $(A, B) = (128, 256)$ .

Suppose the second factor at (13) is zero. The discriminant in  $r$  is

$$\begin{aligned} & -u^6(8v^6 - 24v^5u^2 + 51v^4u^4 - 62v^3u^6 + 45v^2u^8 - 18vu^{10} + 3u^{12}) \\ & = -u^6(8X^6 + 21u^4X^4 + 6u^8X^2 + u^{12}/16), \quad X = v - u^2/2, \end{aligned}$$

which is negative except when  $u = 0$ , in which case either  $v = 0$  or  $3v^3 = 2r^2$ . The former leads to the parametrization as stated in the Theorem, the latter to  $(A, B) = (-5616, -3888)$ .

□

**Theorem 6.5.** *Suppose  $x^4 + Ax + B$  has a rational root, say  $v$ . If the polynomial  $(x^{16} + Ax^4 + B)/(x^4 - v)$  is reducible, then it has reducibility type  $(6, 6)$ , which occurs when, up to scaling, either (1)  $(A, B)$  are given by (9) in Theorem 6.1, when the sextic factors are cubics in  $x^2$ ; or (2),  $(v, A, B)$  is one of the following eight cases:*

$$\begin{aligned} & (72, -347004, -1889568), \quad (-4, 1088, 4096), \quad (540, -49968576, -58047528960), \\ & (1500, -2975000000, -600000000000), \\ & (1234620, -1767811196564438976, -140874409936505522810880), \\ & (-333000, 49083580251562500, 4048461902770312500000), \\ & (1506456, -718119113273864316, -4068405448481125418940000) \\ & (3749256176, -52702993391145847275486817276, -29085892289306030859388663640000). \end{aligned}$$

*Proof.* If the polynomial  $x^{16} + Ax^4 + B$  is divisible by  $x^4 - v$ , then  $B = -Av - v^4$  and

$$(x^{16} + Ax^4 + B)/(x^4 - v) = x^{12} + vx^8 + v^2x^4 + v^3 + A = f(x^4), \text{ say.}$$

Lemma 29 from [3] tells us that either (1)  $f(x^4) = -g(x^2)g(-x^2)$  for a cubic polynomial  $g$ , which leads to the values of  $(A, B)$  as in Theorem 6.1 (and the sextic  $g(x^2)$  is irreducible, as before); or (2),  $f(-4x^4) = cg(x)g(-x)g(ix)g(-ix)$ , with  $c$  constant and  $g(x) \in \mathbb{Z}[x]$  of degree 3. Thus we obtain

$$-64x^{12} + 16vx^8 - 4v^2x^4 + v^3 + A = 64g(x)g(-x)g(ix)g(-ix),$$

where  $g(x) = x^3 + px^2 + qx + r$ , say. This gives

$$-64x^{12} + 16vx^8 - 4v^2x^4 + v^3 + A = 64G(x^2)G(-x^2),$$



where  $G(X) = X^3 + (p^2 - 2q)X^2 + (2pr - q^2)X + r^2$ . Equating coefficients of powers of  $X$  and eliminating  $v$  gives

$$2(p^2 - 2q)(p^8 - 4p^6q + 4p^4q^2 - 3q^4) = (2(7p^2 - 2q)r + 4p^5 - 16p^3q + 10pq^2)^2.$$

and on setting  $X/Z^2 = 6(2q/p^2 - 1)$ , where  $X, Z \in \mathbb{Z}$  and  $(X, Z^2) = 1$ , there results

$$C : X(X^4 + 24X^3Z^2 + 24X^2Z^4 + 864XZ^6 + 1296Z^8) = Y^2.$$

We shall show that the set of rational points on  $C$  comprises precisely the point at infinity, with  $Z = 0$ , and the set:

$$(X/Z^2, \pm Y) = (-18, 864), (6, 288), (0, 0), (-2, 32), (1, 47), (36, 10152).$$

These points return the trinomials listed in the second statement of the Theorem. Certainly  $X = du^2$  with  $d \mid 6$ , so  $d = \pm 1, \pm 2, \pm 3, \pm 6$ . Then

$$X = du^2, \quad X^4 + 24X^3Z^2 + 24X^2Z^4 + 864XZ^6 + 1296Z^8 = dv^2,$$

and the quartic is locally unsolvable for  $d = -1, 2, 3, -6$ . When  $d = -3, 6$ , the quartic is an elliptic curve of rank 0, and the only solutions are given by  $(X, Z^2) = (6, 1)$ ,  $(u, v) = (1, 48)$ . It remains to deal with  $d = 1, -2$ .

Case I:  $d = 1$ :

$$X = u^2, \quad X^4 + 24X^3Z^2 + 24X^2Z^4 + 864XZ^6 + 1296Z^8 = v^2,$$

so that

$$u^8 + 24u^6Z^2 + 24u^4Z^4 + 864u^2Z^6 + 1296Z^8 = v^2.$$

Over  $\mathbb{Q}(\sqrt{3})$ ,

$$(u^4 + (12 + 8\sqrt{3})u^2Z^2 + 36Z^4)(u^4 + (12 - 8\sqrt{3})u^2Z^2 + 36Z^4) = v^2;$$

and the gcd of the two factors on the left can be divisible only by  $(1 + \sqrt{3})$ ,  $(\sqrt{3})$ . Thus

$$u^4 + (12 + 8\sqrt{3})u^2Z^2 + 36Z^4 = \pm(2 + \sqrt{3})^i(1 + \sqrt{3})^j(\sqrt{3})^k\Box.$$

Taking norms,  $v^2 = (-2)^j(-3)^k\Box$ , so that  $j = k = 0$ , and

$$u^4 + (12 + 8\sqrt{3})u^2Z^2 + 36Z^4 = \delta\Box, \quad \delta = \pm(2 + \sqrt{3})^i.$$

Of the four possibilities for  $\delta$ , only  $\delta = 1$  gives a curve locally solvable above 2; and in fact the curve is elliptic with rank 1. The Magma routines work successfully, delivering the points  $(u, Z) = (1, 0), (0, 1), (1, 1), (6, 1)$ .

Case II:  $d = -2$ :

$$X = -2u^2, \quad X^4 + 24X^3Z^2 + 24X^2Z^4 + 864XZ^6 + 1296Z^8 = -2v^2,$$

so that

$$u^8 - 12u^6Z^2 + 6u^4Z^4 - 108u^2Z^6 + 81Z^8 = -2V^2.$$

Over  $\mathbb{Q}(\sqrt{3})$ ,

$$(u^4 + (-6 - 4\sqrt{3})u^2Z^2 + 9Z^4)(u^4 + (-6 + 4\sqrt{3})u^2Z^2 + 9Z^4) = -2V^2,$$

and the gcd of the two factors on the left can be divisible only by  $(1 + \sqrt{3})$ ,  $(\sqrt{3})$ . Thus

$$u^4 + (-6 - 4\sqrt{3})u^2Z^2 + 9Z^4 = \pm(2 + \sqrt{3})^i(1 + \sqrt{3})^j(\sqrt{3})^k\Box.$$

Taking norms,  $-2V^2 = (-2)^j(-3)^k\Box$ , so that  $(j, k) = (1, 0)$ , with

$$u^4 + (-6 - 4\sqrt{3})u^2Z^2 + 9Z^4 = \delta\Box, \quad \delta = \pm(2 + \sqrt{3})^i(1 + \sqrt{3}).$$

Of the four possibilities for  $\delta$ , only  $\delta = -(2 + \sqrt{3})(1 + \sqrt{3})$  gives a curve locally solvable above 2, and in fact an elliptic curve of rank 1. The Magma routines work successfully, delivering the points  $(u, Z) = (1, 1), (3, 1)$ .  $\square$

**Theorem 6.6.** *The trinomial  $x^{15} + Ax^3 + B$  is reducible if and only if either  $x^5 + Ax + B$  is reducible or up to scaling  $(A, B) = (-81, 216), (270, 729)$  with*

$$\begin{aligned} x^{15} - 81x^3 + 216 &= (x^5 + 3x^4 + 6x^3 + 9x^2 + 9x + 6) \times \\ &\quad (x^{10} - 3x^9 + 3x^8 - 6x^5 + 9x^4 - 9x^3 + 27x^2 - 54x + 36), \\ x^{15} + 270x^3 + 729 &= (x^5 + 3x^4 + 6x^3 + 9x^2 + 12x + 9) \times \\ &\quad (x^{10} - 3x^9 + 3x^8 - 3x^6 + 9x^5 - 18x^4 + 63x^2 - 108x + 81). \end{aligned}$$

*Proof.* If  $x^{15} + Ax^3 + B$  is reducible and  $x^5 + Ax + B$  is irreducible, then by Lemma 29 in [3] we know that

$$x^{15} + Ax^3 + B = f(x)f(\zeta_3x)f(\zeta_3^2x),$$

where  $f(x) = x^5 + px^4 + qx^3 + rx^2 + sx + t$ . Expanding the right hand side and equating coefficients:

$$A = s^3 - 3rst + 3qt^2, \quad B = t^3, \quad p^3 - 3pq + 3r = 0,$$

$$r^3 - 3qrs + 3ps^2 + 3q^2t - 3prt - 3st = 0, \quad q^3 - 3pqr + 3r^2 + 3p^2s - 3qs - 3pt = 0.$$

Eliminating  $r, s$ , noting that  $q = p^2$  leads to  $B = 0$ , we get

$$\begin{aligned} &\left( \frac{(2q - p^2)(2p^6 - 6p^4q + 9p^2q^2 - 3q^3) - 18pqt}{(p^2 - q)} \right)^2 \\ &= (p^2 - 2q)(4p^{10} - 24p^8q + 60p^6q^2 - 72p^4q^3 + 45p^2q^4 - 18q^5). \end{aligned}$$

The restriction  $p^2 = 2q$  leads to trivial solutions; and thus the problem of reducibility of  $x^{15} + Ax^3 + B$  reduces to finding all rational points on the genus two curve

$$C : (p^2 - 2q)(4p^{10} - 24p^8q + 60p^6q^2 - 72p^4q^3 + 45p^2q^4 - 18q^5) = 0,$$

where we can assume without loss of generality that  $(p^2, q) = 1$ . We show that the finite points comprise precisely the following set:  $(p^2, q) = (1, 0), (1, 2), (1, 2/3)$ , which lead to the factorizations displayed in the statement of the Theorem. Set  $q/p^2 = (X - 4Z^2)/(2X)$ ,  $X/Z^2 = 4p^2/(p^2 - 2q)$ , so that the equation of the curve takes the form

$$X^5 + 9X^4Z^2 - 48X^3Z^4 + 864X^2Z^6 + 2304Z^{10} = Y^2.$$

The quintic has precisely one real root  $\theta_0$  for  $X/Z^2$ ,  $\theta_0 \sim -15.63983$ , and thus  $Y^2 \geq 0$  implies  $X/Z^2 \geq \theta_0$ . Set  $K = \mathbb{Q}(\theta)$  where  $\theta^5 + 2\theta^4 + 4\theta^3 + 4\theta^2 + 2\theta + 4 = 0$ . The ring of integers is  $\mathbb{Z}[1, \theta, \theta^2, \theta^3, \theta^4/2]$ , and the class number is 1. Fundamental units are given by

$$\epsilon_1 = 1 + 3\theta^2 + \theta^3 + \theta^4, \quad \epsilon_2 = 5 - 3\theta - 6\theta^2 - 4\theta^3 - 2\theta^4,$$

of norm +1. We have the ideal factorizations

$$(2) = p_2p_2', \quad (3) = p_3^5, \quad (5) = p_5^2p_5', \quad \text{Norm}(p_5) = 5, \quad \text{Norm}(p_5') = 5^3.$$

Now

$$\text{Norm}_{K/\mathbb{Q}}(X + 1/2(5\theta^4 + 8\theta^3 + 20\theta^2 + 12\theta + 10)Z^2) = Y^2,$$

and it may be checked that a prime ideal dividing  $X + 1/2(5\theta^4 + 8\theta^3 + 20\theta^2 + 12\theta + 10)Z^2$  to an odd power must be one of  $p_2' = (q_2') = (1 - \theta + \theta^2 + \theta^4/2)$ ,

$p_3 = (q_3) = (-1 - \theta)$ ,  $p_5 = (q_5) = (1 + \theta^2)$ . Thus with  $\delta = \pm \epsilon_1^i \epsilon_2^j q_2'^k q_3^m q_5^n$ ,  $i, j, k, m, n = 0, 1$ , it follows that

$$X + 1/2(5\theta^4 + 8\theta^3 + 20\theta^2 + 12\theta + 10)Z^2 = \delta^{-1}a^2,$$

$$X^4 + 1/2(-5\theta^4 - 8\theta^3 - 20\theta^2 - 12\theta + 8)X^3Z^2 + (-2\theta^4 - 32\theta^3 - 48\theta^2 - 104\theta - 80)X^2Z^4 \\ + (72\theta^4 + 192\theta^3 + 96\theta^2 + 96\theta + 192)XZ^6 + (-96\theta^4 - 384\theta)Z^8 = \delta b^2,$$

with integers  $a, b$  of  $K$  satisfying  $q_2'^k q_3^m q_5^n ab = Y$ . Taking norms,  $Y^2 = 2^k 3^m 5^n \square$ , so that  $k = m = n = 0$ . Further,  $\epsilon_1, \epsilon_2$  evaluated at  $\theta_0$  are approx. 8.399 and 0.3477: so are positive. Thus  $X/Z^2 \geq \theta_0 = -1/2(5\theta^4 + 8\theta^3 + 20\theta^2 + 12\theta + 10)$  implies the negative sign cannot hold. Hence in particular

$$X^4 + 1/2(-5\theta^4 - 8\theta^3 - 20\theta^2 - 12\theta + 8)X^3Z^2 + (-2\theta^4 - 32\theta^3 - 48\theta^2 - 104\theta - 80)X^2Z^4 \\ + (72\theta^4 + 192\theta^3 + 96\theta^2 + 96\theta + 192)XZ^6 + (-96\theta^4 - 384\theta)Z^8 = \epsilon_1^i \epsilon_2^j b^2,$$

with  $ab = Y$ . The quartic curve is everywhere locally solvable if and only if  $\delta = 1, \epsilon_1$ .

Case I:  $\delta = 1$ . Now we have

$$C_1 : X^4 - 1/2(5\theta^4 + 8\theta^3 + 20\theta^2 + 12\theta - 8)X^3Z^2 - (2\theta^4 + 32\theta^3 + 48\theta^2 + 104\theta + 80)X^2Z^4 \\ + (72\theta^4 + 192\theta^3 + 96\theta^2 + 96\theta + 192)XZ^6 + (-96\theta^4 - 384\theta)Z^8 = b^2.$$

The equation is that of an elliptic curve of rank 3, and the Magma routines show that the only points on  $C_1$  with  $X/Z^2 \in \mathbb{Q}$  are given by  $(X, Z^2) = (1, 0), (0, 1)$ .

Case II:  $\delta = \epsilon_1$ . Now we have

$$C_2 : X^4 + 1/2(-5\theta^4 - 8\theta^3 - 20\theta^2 - 12\theta + 8)X^3Z^2 + (-2\theta^4 - 32\theta^3 - 48\theta^2 - 104\theta - 80)X^2Z^4 \\ + (72\theta^4 + 192\theta^3 + 96\theta^2 + 96\theta + 192)XZ^6 + (-96\theta^4 - 384\theta)Z^8 = \epsilon_1 b^2,$$

with point at  $(X, b, Z^2) = (4, -32\theta^3 - 32\theta^2 - 32\theta - 64, 1)$ . The curve is elliptic with  $K$ -rank 3; and the Magma routines work satisfactorily to show that the only points on  $C_2$  with  $X/Z^2 \in \mathbb{Q}$  are  $(X, Z^2) = (4, 1), (-12, 1)$ .  $\square$

## 7. CONCLUDING REMARKS AND SOME NEW SPORADIC TRINOMIALS

Generalizing a statement in Theorem 2.1, we have the following result.

**Theorem 7.1.** *There are no trinomials  $x^n + Ax + B$ ,  $n$  even, with three linear factors.*

*Proof.* By considering the four possibilities for sign of  $A, B$ , it follows immediately from Descartes' Rule of Signs that the polynomial  $x^n + Ax + B$ ,  $n$  even, can have at most two real roots; and the assertion of the Theorem follows.  $\square$

**Remark 7.2.** This argument applies over any real field, so that reducibility type  $(1, 1, 1, n - 3)$  is impossible for trinomials  $x^n + Ax + B$ ,  $n$  even, defined over any real field.

When  $n$  is odd, let  $p, q, r$  be distinct rational roots of  $x^n + Ax + B$  (where now Descartes' Rule of Sign implies  $A < 0$ ). Then

$$p^n + Ap + B = 0, \quad q^n + Aq + B = 0, \quad r^n + Ar + B = 0,$$

and eliminating  $A, B$ ,

$$(q - r)p^n + (r - p)q^n + (p - q)r^n = (p - q)(q - r)(r - p)G_n(p, q, r) = 0.$$

The equation  $G_n(p, q, r)$  (which represents a curve of genus  $(n-4)(n-3)/2$ ) has indeed (trivial) points, but we do not know how to show these trivial points form the complete set of solutions, which we believe to be the case. Indeed, we firmly believe that the following conjecture is true.

**Conjecture 7.3.** *Let  $n \geq 4$ . There are no trinomials  $x^n + Ax + B$  defined over  $\mathbb{Q}$  with reducibility type  $(1, 1, 1, n-3)$ .*

Finally, while studying the trinomials of this paper, the following sporadic trinomial factorizations came to light, and do not appear to have been previously recorded:

trinomial	factor
$x^9 + 27x^4 - 108$	$x^3 + 3x^2 + 6x + 6$
$x^{10} + 297x^3 + 648$	$x^5 + 3x^3 + 9x^2 - 9x + 18$
$x^{11} + 12x + 8$	$x^5 - 2x^4 + 2x^3 - 2x^2 + 2$
$x^{11} - 6184976x^3 + 4216540160$	$x^3 + 14x^2 + 98x + 392$
$x^{13} - 340224x + 732160$	$x^3 - 2x^2 + 8x - 20$
$x^{16} + 3486328125x + 9277343750$	$x^3 + 5x^2 + 25x + 50$
$x^{16} + 34816x^3 - 552960$	$x^4 + 2x^3 - 8x - 24.$

**Acknowledgements:** We are grateful to the referee for a careful reading of the original manuscript, and for helpful suggestions. All computations in this paper were carried out using Magma [1]. The research of the second author was supported by Polish Government funds for science, grant I 2010 044 770 for the years 2010–2011.

#### REFERENCES

- [1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235-265, 1997.
- [2] L. J. Mordell, *Diophantine equations*, Academic Press, London, 1969.
- [3] A. Schinzel, *On reducible trinomials*, Dissertationes Mathematicae, CCCXXIX, Warsaw, 1993.
- [4] A. Schinzel, *On reducible trinomials, II*, Publ. Math. Debrecen **56/3-4** (2000), 575-608.
- [5] A. Schinzel, *On reducible trinomials, III*, Period. Math. Hung. **43** (1-2) (2001), 43-69.
- [6] A. Schinzel, *Selecta*, Volume I: Diophantine problems and polynomials. Volume II: Elementary, analytic and geometric number theory. Edited by Henryk Iwaniec, Władysław Narkiewicz and Jerzy Urbanowicz. Heritage of European Mathematics. Zürich: European Mathematical Society Publishing House (EMS).
- [7] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

School of Mathematics and Statistical Sciences, Arizona State University, Tempe AZ 85287-1804, USA; e-mail: bremner@asu.edu,

Jagiellonian University, Faculty of Mathematics and Computer Science, Institute of Mathematics, Łojasiewicza 6, 30-348 Kraków, Poland; email: Maciej.Ulas@im.uj.edu.pl